UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

LATASHA BROOKS and **MICHAEL BROOKS,** on behalf of themselves and all others similarly situated, Plaintiffs, v. **PEOPLES BANK, as successor by merger to LIMESTONE BANK, INC.,** Defendant.	Case No. Judge Magistrate Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Latasha Brooks and Michael Brooks ("Plaintiffs") bring this Class Action Complaint against Defendant Peoples Bank ("Defendant" or "Peoples"), in their individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendant Peoples Bank is an Ohio corporation and chartered commercial bank, with 132 full-service branch locations in Ohio, Kentucky, West Virginia, Virginia, Washington D.C., and Maryland.[1] It offers a broad range of services including financing services, investment and money management services, leasing services, and insurance services, along with other general personal and business banking services.[2]

[1] https://www.peoplesbancorp.com/about-us/about-peoples?scrollToContent=true (last visited September 21, 2023).
[2] *Id.*

2. Peoples is the successor by merger to Limestone Bank, Inc. ("Limestone"), a former Kentucky banking corporation which merged with and into Peoples on April 30, 2023. Therefore, the term "Defendant" in this Complaint shall be interpreted as referring to Limestone in all averments relating to events that took place prior to this merger.

3. Plaintiffs bring this class action against Defendant for Limestone's failure to properly secure and safeguard Personally Identifiable Information ("PII") and Protected Health Information ("PHI," together with PII "Private Information") provided by its clients, including, without limitation, Social Security numbers, drivers' license numbers, financial account information, and medical information.

4. At an undisclosed point in time, Defendant identified that between November 21, 2022, and March 23, 2023, unauthorized third parties were able to access Limestone's network and computer system through an unsecure employee email address. An investigation "found evidence of unauthorized access" on this email account which had access to and contained Private Information from Limestone's network (the "Data Breach").[3]

5. Defendant failed to use reasonable industry standard security measures, which would have prevented this type of attack from being successful. Defendant's failure to use such measures is particularly egregious given the amount of highly sensitive Private Information that it maintains and the prevalence of data security incidents in the finance and banking industries.

6. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Hackers can access and then offer for sale the unencrypted, unredacted Private

[3] https://www.peoplesbancorp.com/about-us/limestone-bank/limestone-security-incident-notice (last visited September 21, 2023).

Information to criminals. The exposed Private Information of Plaintiffs and Class Members can be sold on the dark web. Plaintiffs and Class Members now face a present and continuing lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. Plaintiffs brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

9. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption

of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to a known criminal organization. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Latasha Brooks

11. Plaintiff Latasha Brooks is, and at all times relevant has been, a resident and citizen of Beaver Dam, Kentucky. Plaintiff received a "Notice of Data Breach" letter dated September 15, 2023, on or about that date. The letter notified Plaintiff that between November 21, 2022, and March 23, 2023, an unauthorized actor was able to access Plaintiff's Private Information through a compromised employee email account. The type of data and information at issue included Plaintiff's name, financial account number, and Social Security number. The letter further advised that Plaintiff should "remain vigilant by reviewing your financial account statements and credit reports for any unauthorized activity."

Plaintiff Michael Brooks

12. Plaintiff Michael Brooks is, and at all times relevant has been, a resident and citizen of Beaver Dam, Ohio County, Kentucky. Plaintiff received a "Notice of Data Breach" letter dated September 15, 2023, on or about that date. The letter notified Plaintiff that between November 21, 2022, and March 23, 2023, an unauthorized actor was able to access Plaintiff's Private Information through a compromised employee email account. The type of data and information at issue included Plaintiff's name, financial account number, and Social Security number. The letter further advised that Plaintiff should "remain vigilant by reviewing your financial account statements and credit reports for any unauthorized activity."

Defendant Peoples Bank

13. Defendant Peoples Bank is an Ohio corporation and chartered commercial bank with its principal office located at 138 Putnam St., Marietta, OH 45750. It operates 132 full-service branch locations throughout Ohio, Kentucky, West Virginia, Virginia, Washington D.C., and Maryland.

14. Limestone Bank, Inc., a former Kentucky banking corporation, merged with and into Peoples Bank on April 30, 2023, at which point its corporate existence ceased and "all debts, liabilities and duties of Limestone…bec[a]me obligations of [Peoples], and may [now] be enforced against it to the same extent as if such debts, liabilities and duties had been incurred or contracted by it."[4] Plaintiffs' claims stated herein are therefore asserted against Defendant as successor by merger to Limestone Bank, Inc.

15. At the time of filing its Articles of Merger with the Kentucky Secretary of State, Peoples also adopted "Limestone Bank, Inc." as an assumed name for use in the Commonwealth of Kentucky with effect from May 1, 2023, and therefore all actions taken in the name of Limestone Bank, Inc., on and after that date have been taken by Defendant Peoples directly.[5]

JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the

[4] Articles of Merger of Limestone Bank, Inc., a Kentucky Banking Corporation, with and into Peoples Bank, an Ohio Chartered Commercial Bank, Ex. A (Form of Agreement and Plan of Merger), at Agreements, § 9 (Apr. 28, 2023), filed with the Kentucky Secretary of State and available at his official website here: https://web.sos.ky.gov/corpscans/84/0950084-09-99999-20230428-9585781-PU.pdf (last visited September 21, 2023).

[5] Certificate of Assumed Name (Apr. 28, 2023) filed with the Kentucky Secretary of State and available at his official website here: https://web.sos.ky.gov/corpscans/84/0950084-09-99999-20230428-9585697-PU.pdf (last visited September 21, 2023).

proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

17. The U.S. District Court for the Southern District of Ohio has personal jurisdiction over Defendant named in this action because Defendant has its principal place of business in Washington County in this District, and Defendant conducts substantial business in Ohio and this District through its headquarters, other offices, parent, and affiliates.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and its parent or affiliates are headquartered in this District and Division, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Background

19. Defendant Peoples Bank is a bank headquartered in Marietta, Ohio. According to its website, it holds nearly $9 billion in total assets, consists of 132 operating full-service bank branch locations, and employs more than 1,500 associates.

20. As of March 31, 2023, Limestone had approximately $1.5 billion in total assets, and operated 20 branches throughout Kentucky.[6]

21. Plaintiffs and the Class Members, as current or former customers of Limestone, reasonably relied (directly or indirectly) on this sophisticated company to keep their sensitive Private Information confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information. It is common sense that customers expect reasonable security when entrusting a company with highly sensitive Private Information like a combination of their Social Security numbers, drivers' license

[6] https://www.prnewswire.com/news-releases/peoples-bancorp-completes-acquisition-of-limestone-bancorp-301811352.html (last visited September 21, 2023).

numbers, financial account information, and medical information.

22. Limestone had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

The Data Breach

23. On or around September 15, 2023, Defendant began notifying certain Class Members of the Data Breach.[7] It also posted notice to its website.

24. Defendant's notice to Class Members informs them that:

> Limestone identified unusual activity involving an employee's email account. Upon learning of this, Limestone immediately took steps to secure the email account and began an investigation. A cybersecurity firm was engaged to assist. The investigation found evidence of unauthorized access to one employee email account between November 21, 2022 and March 23, 2023.
>
> The emails and files in this account were reviewed, and Limestone determined that some contained personal information. The information varied, but depending on the person, the information may have included name and one or more of the following: Social Security number, driver's license number, financial account information, and limited medical information.[8]

25. The notice posted to Defendant's website states that the following information of the recipients was compromised in the Data Breach: "Social Security number, driver's license number, financial account information, and limited medical information."

26. The letters received by Plaintiffs similarly informed them that their information was compromised:

> Limestone identified unusual activity involving an employee's email account and immediately took steps to secure the account and began an investigation. A cybersecurity firm was engaged to assist. The investigation found evidence of unauthorized access to one employee email account between November 21, 2022, and March 23, 2023. The email and files in this account were reviewed, and

[7] https://www.peoplesbancorp.com/about-us/limestone-bank/limestone-security-incident-notice (last visited September 21, 2023).
[8] *Id.*

> Limestone determined that at least one email or file contained your name and Social Security number and financial account number.[9]

27. In its data breach notice letters to Plaintiffs and Class Members, Defendant recognized the substantial risk of imminent harm presented by the Data Breach. Defendant instructed the victims of the Data Breach to "remain vigilant" and offered to provide victims with one year of credit monitoring services. However, this is inadequate to compensate Plaintiffs and Class Members, who will face a substantial risk of harm for the rest of their lives.

Securing Private Information and Preventing Breaches

28. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

29. In its notice letters, Defendant acknowledged the sensitive and confidential nature of Private Information. To be sure, collection, maintaining, and protecting Private Information is vital to virtually all of Defendant's business purposes. Defendant acknowledged through its conduct and statements that the misuse or inadvertent disclosure of Private Information can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect Private Information from improper release or disclosure.

30. Defendant's Privacy Statement, posted on its website, states in bold and certain terms "We promise to protect your privacy" and "We promise to secure your information."[10]

31. Defendant further assures its clients and customers that "Peoples Bank does not share nonpublic information about you with third-party marketers outside of the Peoples family of

[9] September 15, 2023, Data Breach Notice Letter to Michael Brooks.
[10] https://www.peoplesbancorp.com/about-us/privacy-and-security/ (last visited September 21, 2023)

companies without your consent, except as explained in the enclosed notice."[11]

32. In concluding its Privacy Statement, Defendant expresses: "Security of information is a top priority for the Peoples family of companies. We comply with federal standards to protect your information through physical, electronic, and procedural safeguards."[12]

33. Defendant had a duty to adopt reasonable measures to protect and secure Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

The Cyber Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

34. It is well known that Private Information, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

35. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[13]

36. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[14]

37. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[15]

38. Individuals place a high value not only on their Private Information, but also on the

[11] *Id.*
[12] *Id.*
[13] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf, at 2 (last accessed Sept. 21, 2023)
[14] *Id.*
[15] *Id.*

privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

39. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

40. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

41. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times Defendant Had a Duty to Plaintiffs and Class Members to Properly Secure their Private Information

42. At all relevant times, Defendant had a duty to Plaintiffs and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to *promptly* notify Plaintiffs and Class Members when it became aware that their Private Information may have been compromised.

43. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Limestone, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the Members of the Class entrusted Limestone with their Private Information when they were customers of Limestone.

44. Limestone had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Limestone breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

45. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

46. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

47. The ramifications of Limestone's failure to keep its Class Members' Private Information secure are long lasting and severe. Once PII is stolen, particularly financial information, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Private Information

48. PII of data breach victims remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id*.
[18] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Sept. 21, 2023).

value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[19]

49. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[20]

50. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[21]

51. Given the nature of Defendant's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII may easily obtain Plaintiffs' and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

52. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[22] The

---

[19] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed Sept. 21, 2023).

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Sept. 21, 202).

[21] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[22] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*:

information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

53. To date, Defendant has only offered its Class Members basic credit monitoring services even with the delay from their discovery of the Data Breach to the production of the notice letters. The advice offered to victims in the notice letters is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

54. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Class Members.

Defendant Failed to Comply with FTC Guidelines

55. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

56. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Sept. 21, 2023).

e. implement policies to correct security problems.

57. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

58. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Plaintiffs and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

61. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class Members provided Defendant with sensitive personal information, including their private financial information.

62. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiffs and other reasonable

Class Members understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

63. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiffs has also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

64. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, contact information, financial information, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

65. In addition, if a Class Member's PII is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

66. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction

and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

67. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[23]

68. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[24] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[25] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

69. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages.

70. In its notice letter, Defendant represented to the Class Members that the vulnerability lasted from November 2022 through March 2023 and admitted files were fully accessible by cybercriminals. Though Defendant said nothing about exfiltration of data, as

---

[23] *Id.*

[24] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), https://www.susanladika.com/freelance_writer_susan_ladika_personal_finance_data_breaches_pose_a_greater_risk.html (last accessed September 21, 2023).

[25] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://javelinstrategy.com/research/consumer-data-insecurity-report) (last accessed September 21, 2023).

EmiSoft, an award-winning malware-protection software company, states "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, *especially during the preliminary stages of the investigation*."[26] It is likely that the cybercriminals did steal data and did so undetected.

71. In this case, according to Defendant's notification to the Class Members, cybercriminals had access to Class Members' data at least on November 21, 2022, its notice letters about that Data Breach did not go out until September 15, 2023. This is tantamount to the cybercriminals having ten month a head start on stealing the identities of Plaintiffs and Class Members.

72. Accordingly, that Defendant has not found evidence of data being viewed is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Michael Brooks's Experience

73. Plaintiff Michael Brooks provided his Private Information to Limestone as a condition of receiving financial and banking services.

74. Plaintiff Michael Brooks is very careful about sharing his Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff Michael Brooks stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique

[26] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EmiSoft Blog July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last accessed September 21, 2023, emphasis added)).

usernames and passwords for his various online accounts.

75. Plaintiff reasonably relied on Limestone, a sophisticated company, to protect the security of his Private Information. Plaintiff would not have entrusted Limestone with his Private Information had he had known Limestone would not exercise reasonable care.

76. On or about September 15, 2023, Plaintiff Michael Brooks received a Notice of Data Security Incident Letter by US. Mail. The letter stated:

> Limestone identified unusual activity involving an employee's email account and immediately took steps to secure the account and began an investigation. A cybersecurity firm was engaged to assist. The investigation found evidence of unauthorized access to one employee email account between November 21, 2022, and March 23, 2023. The email and files in this account were reviewed, and Limestone determined that at least one email or file contained your name and Social Security number and financial account number.[27]

77. As a result of the Data Breach and the information that he received in the notice letter, Plaintiff Michael Brooks has spent hours dealing with the consequences of the Data Breach (changing passwords, and self-monitoring bank and credit accounts), as well as his time spent verifying the legitimacy of the written correspondence, communicating with his bank, exploring credit monitoring and identity theft insurance options, and signing up for the credit monitoring. This time has been lost forever and cannot be recaptured.

78. Plaintiff Michael Brooks suffered actual injury in the form of damages and diminution in the value of his Private Information —a form of intangible property that he entrusted to Limestone, which was compromised in and as a result of the Data Breach.

79. Plaintiff Michael Brooks has suffered injury from a loss of privacy.

80. As a result of the admitted exfiltration of Plaintiff Michael Brooks's name, Social Security number, and financial account information by cybercriminals, Plaintiff Michael Brooks

[27] September 15, 2023, Data Breach Notice Letter to Michael Brooks.

faces a substantial risk of imminent fraud, identity theft, and misuse of Private Information.

81. Plaintiff Michael Brooks has suffered annoyance, inconvenience, anxiety, mental stress, mental anguish, and emotional distress as a result of the Data Breach, loss of privacy, and the substantial risk of imminent harm.

82. As a result of Limestone's continued failure to implement and maintain reasonable security measures, Plaintiff Michael Brooks may face a substantial risk of imminent harm from future data breaches. Because data breaches entail a loss of privacy and the information at risk (e.g., names, Social Security numbers, and financial account information) is largely static, any injury to Plaintiff Michael Brooks from future Data Breaches will be irreparable. Plaintiff Michael Brooks has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches, and upon information and belief, this remains backed up on Limestone's legacy systems, though now under Defendant Peoples' control.

Plaintiff Latasha Brooks's Experience

83. Plaintiff Latasha Brooks provided her Private Information to Limestone as a condition of receiving financial and banking services.

84. Plaintiff Latasha Brooks is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff Latasha Brooks stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

85. Plaintiff reasonably relied on Limestone, a sophisticated company, to protect the

security of her Private Information. Plaintiff would not have entrusted Limestone with her Private Information had she had known Limestone would not exercise reasonable care.

86. On or about September 15, 2023, Plaintiff Latasha Brooks received a Notice of Data Security Incident Letter by US. Mail. The letter stated:

> Limestone identified unusual activity involving an employee's email account and immediately took steps to secure the account and began an investigation. A cybersecurity firm was engaged to assist. The investigation found evidence of unauthorized access to one employee email account between November 21, 2022, and March 23, 2023. The email and files in this account were reviewed, and Limestone determined that at least one email or file contained your name and Social Security number and financial account number.[28]

87. As a result of the Data Breach and the information that she received in the notice letter, Plaintiff Latasha Brooks has spent hours dealing with the consequences of the Data Breach (changing passwords, and self-monitoring bank and credit accounts), as well as time spent verifying the legitimacy of the written correspondence, communicating with her bank, exploring credit monitoring and identity theft insurance options, and signing up for the credit monitoring. This time has been lost forever and cannot be recaptured.

88. Plaintiff Latasha Brooks suffered actual injury in the form of damages and diminution in the value of his Private Information — a form of intangible property that she entrusted to Limestone, which was compromised in and as a result of the Data Breach.

89. Plaintiff Latasha Brooks has suffered injury from a loss of privacy.

90. As a result of the admitted exfiltration of Plaintiff Latasha Brooks's name, Social Security number, and financial account information by cybercriminals, Plaintiff Latasha Brooks faces a substantial risk of imminent fraud, identity theft, and misuse of Private Information.

91. Plaintiff Latasha Brooks has suffered annoyance, inconvenience, anxiety, mental

[28] September 15, 2023, Data Breach Notice Letter to Latasha Brooks.

stress, mental anguish, and emotional distress as a result of the Data Breach, loss of privacy, and the substantial risk of imminent harm.

92. As a result of Limestone's continued failure to implement and maintain reasonable security measures, Plaintiff Latasha Brooks may face a substantial risk of imminent harm from future data breaches. Because data breaches entail a loss of privacy and the information at risk (e.g., names, Social Security numbers, and financial account information) is largely static, any injury to Plaintiff Latasha Brooks from future Data Breaches will be irreparable. Plaintiff Latasha Brooks has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches, and upon information and belief, this remains backed up on Limestone's legacy systems, though now under Defendant Peoples' control.

CLASS ALLEGATIONS

93. Plaintiffs bring the following nationwide class action on behalf of themselves and all others similarly situated.

> **All persons residing in the United States whose Private Information was compromised in the Data Breach announced by Limestone Bank, Inc., in its September 15, 2023, Notice Letter (the "Class").**

94. Excluded from the Class are the following individuals and/or entities: Peoples Bank, and its parents, subsidiaries, affiliates, officers and directors, and any entity in which Peoples has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

95. Plaintiffs reserve the right to modify or amend the definition of the proposed class

and any future subclass before the Court determines whether certification is appropriate.

96. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

97. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

98. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

99. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

100. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent

and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

101. Predominance, Fed. R. Civ. P. 23(b)(3): Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

102. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

103. The nature of this action and the nature of laws available to Plaintiffs and Class

Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

104. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

105. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

106. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

107. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

108. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether a contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

g. Whether Defendant breached the implied contract;

h. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their P Private Information II had been compromised;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

109. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

110. As a condition of receiving services from Defendant, Defendant's current and former customers were obligated to provide Defendant with their Private Information or the Private Information of their employees, including, but not limited to Social Security numbers, drivers' license numbers, financial account information, and medical information.

111. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

112. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

113. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

114. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

115. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information that Defendant was no longer required to retain pursuant to regulations or legitimate business purposes.

116. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

117. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant on the one hand and Plaintiffs and the Class on the other. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part receiving services from Defendant.

118. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

119. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

120. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting

Private Information stored on Defendant's systems.

121. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

122. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

123. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

124. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

125. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

126. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

127. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the

Private Information was within Defendant's possession or control.

128. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

129. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and the Class in the face of increased risk of theft.

130. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' Private Information.

131. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

132. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

133. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the present harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

134. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the

loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

135. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

136. Additionally, as a direct and proximate result of Defendant's Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

137. Plaintiffs and Class Members are therefore entitled to damages, including

restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

138. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 137.

139. Defendant benefited from receiving Plaintiffs' and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

140. Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

141. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of providing their Private Information to Defendant and Plaintiffs' and Class Members' employers conferred a monetary benefit by purchasing loan services. In connection thereto, Plaintiffs and Class Members and/or their employers provided Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, Plaintiffs and Class Members were required to provide their Private Information. In exchange, Plaintiffs and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

142. Defendant knew Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs

and Class Members for business purposes.

143. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members.

144. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

145. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

146. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

147. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

148. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

149. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information. Such agreement exists anytime there is an exchange of highly sensitive Private Information, such as a combination of names, financial account information, medical information, and Social Security numbers.

150. Defendant solicited and invited Class Members to provide their Private Information Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

151. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards. Plaintiffs and Class Members further understood that Defendant's employees would not use the Private Information to commit crimes against them.

152. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

153. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

154. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

155. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

156. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

157. Plaintiffs and Class Members lost the benefit of their bargain.

158. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

159. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and Class)

160. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 159.

161. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

162. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with its customers, in particular, to keep secure their Private Information.

163. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

164. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

165. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

166. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

167. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

168. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or

harm, and other economic and non-economic losses.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and the Class)

169. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 168.

170. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

171. Defendant owes a duty of care to Plaintiffs and Class Members that requires it to adequately secure Plaintiffs' and Class Members' Private Information.

172. Defendant failed to fulfill its duty of care to safeguard Plaintiffs' and Class Members' Private Information.

173. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

174. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

175. Plaintiffs therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the

following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, customers' and employees' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Peoples Bank and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiffs and their Counsel to represent the certified Class;

B. For equitable relief enjoining Peoples from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' Private Information, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and Class;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: September 21, 2023

Respectfully Submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Spencer D. Campbell (103001)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
scampbell@msdlegal.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 21, 2023, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Terence R. Coates
Terence R. Coates (0085579)